UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/532,434	04/22/2005	Unho Choi	5835-001/NP	9122

27572 7590 04/17/2009
HARNESS, DICKEY & PIERCE, P.L.C.
P.O. BOX 828
BLOOMFIELD HILLS, MI 48303

EXAMINER	
VAUGHAN, MICHAEL R	
ART UNIT	PAPER NUMBER
2431	
MAIL DATE	DELIVERY MODE
04/17/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/532,434	CHOI, UNHO	
	Examiner	Art Unit	
	MICHAEL R. VAUGHAN	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 February 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *2/27/09* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

The instant application having Application No. 10/532434 is presented for examination by the examiner. Claims 1-27 are pending.

Response to Amendment

Drawings

The currently filed drawing are accepted.

Specification

The specification is now accepted.

Response to Arguments

Applicant's arguments filed 2/27/09 have been fully considered but they are not persuasive. Applicant should submit an argument pointing out disagreements with the examiner's contentions. Applicant must also discuss the references applied against the claims, explaining how the claims avoid the references or distinguish from them. Applicant has merely reiterated what the previous Office Action pointed out with respect to the primary reference; specifically the limitation of the independent claim that the primary reference did not teach; and alleged that none of the other cited references taught the missing limitation whether or not they were relied upon to teach it. Merely

saying a reference does not teach without some explanation is not persuasive.

Examiner maintains the previous 103 rejections.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 2, 4, 7-11, 16, 22, 23, and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hrabik et al. (US 2002/0178383 A1) in view of Gleichauf et al. (US 6,324,656 B1).

With respect to claim 1, Hrabik teaches the limitation of "an information collecting/managing section for collecting security information about a wide range of security incidents and vulnerabilities which may be a threat to systems to be protected, via nationwide or enterprise-wide information technology infrastructures, including computer systems or networks, applications and internet services, and storing source data" (page 5, paragraph 0055) as the process preferably starts with collection of disparate events from the target network. To accomplish the above step, the subsystem is provided with a collection engine collecting the event-data from various devices on

the target network. The collection engine receives events from disparate servers and network devices, aggregates the information, and stores it into the event log. The enterprise event analyzer compares events from one enterprise to events from another enterprise (page 6, paragraph 0059).

Further, Hrabik teaches the limitation of "an information processing/analyzing section for processing and analyzing collected security information using a predetermined analysis algorithm and storing and managing analysis results" (page 6, paragraph 0059) as after the events have been consolidated and classified, they enter the correlation stage, which is performed by a hierarchy of event analyzers, which may include a plurality of network event analyzers, an enterprise event analyzer, preferably a part of the security subsystem, and a global event analyzer, preferably a part of the security master system. A network event analyzer analyzes data in various views, described above, looking for events exceeding predetermined thresholds. Event analyzers can also use the results of vulnerability scans to prioritize detected security events.

Furthermore, Hrabik teaches the limitation of "an operating system section including an information sharing/searching/announce unit for transferring the processed and analyzed information to at least one system to be protected or an external system" (page 6, paragraph 0059) the enterprise event analyzer compares events from one enterprise to events from another enterprise.

In addition, Hrabik teaches the limitation of "a display unit for outputting necessary security information in a predetermined form" (page 6, paragraph 0060) as

when an event is uploaded for review by the master system, a single ticket is generated for all security events determined to be related to the same attack and a security engineer begins researching the information in the ticket. It would be obvious to one of the ordinary skill in the art at the time of the invention that for the security engineer to access the information provided in the ticket, it has to be displayed in some form.

Hrabik also teaches the limitation of "an information security section for protecting the integrated computer emergency response system's own information" (page 5, paragraph 0052) as the security system continually determines the effectiveness of e-security defensive measures continual self-checks. The scan dispatcher mechanism forwards particular scan signatures to a system scan analyzer. Events matching predetermined parameters of the system's scan are placed in the scan view upon receipt by the security subsystem. This allows the provided security system to determine if the system is working properly.

It is noted, however, that Hrabik does not explicitly teach the limitation of "a database section including a vulnerability DB for storing vulnerability information and a source/processed DB for storing source data and processed data."

On the other hand, Gleichauf teaches the abovementioned limitation (column 2, lines 11-15) as the information from the collected banners is stored as entries in a first database. Analysis is performed on the entries in the first database by comparing the entries with a rule set to determine potential vulnerabilities. The results of the analysis are then stored in a second database.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Gleichauf into the system of Hrabik to provide better management options for the data collected from collection engine and analyzer engine.

With respect to claim 2, Hrabik teaches the limitation of "an CERT/ISAC/ESM to CERT/ISAC/ESM interworking section for interworking with external systems, including ISACs, CERTs and ESMs, in order to share reliable information" (page 2, paragraph 0018) as a network security system can detect, examine, and respond to security trends and patterns across multiple enterprises.

With respect to claim 4, Hrabik teaches the limitation of "information collecting/managing section includes a vulnerability scanning result collecting unit for periodically scanning vulnerabilities and collecting scanning results" (page 5, paragraph 0055) as the subsystem provided with a collection engine collecting the event-data from various devices on the target network. The collection engine receives events from disparate servers and network devices, aggregates the information, and stores it into the event log.

With respect to claim 7, Hrabik teaches the limitation of "information collecting/managing section includes an incident report collecting unit for receiving security incident reports through communication means, such as telephone, facsimile,

e-mail and web sites, and storing information about reported incidents" (page 6, column 0060) as a single ticket is generated for all security events determined to be related to the same attack, and a security engineer immediately begins researching the information in the ticket.

With respect to claim 8, it is noted that Hrabik does not explicitly teach the limitation of "information collecting/managing section includes a system asset information collecting unit for collecting and normalizing information about systems and network devices involved in the integrated computer emergency response system and asset information relating to the significance (asset values) of the systems and the network devices and storing the collected information."

On the other hand, Gleichauf teaches the abovementioned limitation (column 4, lines 15-28) as NVA engine is operable to ping devices coupled to network backbone in order to identify all such devices or systems that are so coupled. Such an operation can be called "host discovery." NVA engine can, perform port scans on each device coupled to network backbone. NVA engine can further receive banners from the scanned ports. NVA engine can use such banner information to create and to maintain port database.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Gleichauf into the system of Hrabik to provide a network map that can be created to compile the network information.

With respect to claim 9, Hrabik teaches the limitation of "information collecting/managing section includes a collecting and storing in real time events relating to information security from at least one information security product of a firewall (F/W) system, an intrusion detection system (IDS), a policy management system, a anti-virus product, a PC information security system, a retracing system, a PKI certification system, a network device and a virtual private network (VPN) (page 5, paragraph 0055) as the subsystem provided with a collection engine collecting the event-data from various devices on the target network. The collection engine receives events from disparate servers and network devices, aggregates the information, and stores it into the event log.

With respect to claim 10, Hrabik teaches the limitation of "a dataware housing unit for normalizing information collected by the information collecting/managing section in various categories and establishing database storing information" (page 6, paragraph 0056) as once the events have been received, the security system begins consolidating the events. To consolidate security events, each event is compared to a database of system and message "fingerprints" to properly identify the source of the event message. All events are then mapped so that they are presented in the same standardized/normalized format.

In addition, Hrabik teaches the limitation of "an information analyzing unit for analyzing the information stored in the database established by the dataware housing section by applying a data mining or knowledge-based analysis algorithm and an

analysis algorithm for analyzing security incidents and vulnerabilities, correlations with major assets, recognizable patterns and classifications for preventing incidents and vulnerabilities" (page 6, paragraph 0059) as after the events have been consolidated and classified, they enter the correlation stage, which is performed by a hierarchy of event analyzers, which may include a plurality of network event analyzers, an enterprise event analyzer, preferably a part of the security subsystem, and a global event analyzer, preferably a part of the security master system. A network event analyzer analyzes data in various views, described above, looking for events exceeding predetermined thresholds. Event analyzers can also use the results of vulnerability scans to prioritize detected security events.

With respect to claim 11, Hrabik teaches the limitation of "dataware housing unit receives security data, classifies the received information, determines whether the data need be summarized or processed" as taught in claim 10.

It is noted, however, that Hrabik does not explicitly teach the limitation of "dataware housing unit summarizes the data according to search types or adds a data field to generate a database."

On the other hand, Gleichauf teaches the abovementioned limitation (column 2, lines 11-15) as the analysis is performed on the entries in the first database by comparing the entries with a rule set to determine potential vulnerabilities. The results of the analysis are then stored in a second database.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Gleichauf into the system of Hrabik to provide better management options for the security data collected from the system.

With respect to claim 16, Hrabik teaches the limitation of "an asset evaluation/recovery period calculation section for evaluating the significance or asset value of a system to be protected and anticipating damage resulting from a possible security incident and a recovery period based on the evaluated significance of the system" (page 2, paragraph 0021) as it is another object of the present invention to assess the likelihood or impact of an attack by comparing the baseline system information (system configuration, last assessment results, attack history, etc.) to the specific details of the attack. Furthermore, Hrabik teaches (page 7, paragraph 0068) as the master security systems may conduct visibility scans which ensure that port rules changes did not make the target network more vulnerable to attacks. The master system uses a process of baselining to determine a target network's "fingerprint," i.e., the specific view of the target network from the Internet. The master system analyzes these services and preferably separates them into several categories based on the asserted risk to the target network.

With respect to claim 22, Gleichauf teaches a method for responding to a security incident by using an integrated computer emergency response system, which comprises:

an information collecting step performed by an information collecting/managing section to collect security information about security incidents and vulnerabilities through a predetermined communication network (page 5, paragraph 0055) as the process preferably starts with collection of disparate events from the target network. To accomplish the above step, the subsystem is provided with a collection engine collecting the event-data from various devices on the target network. The collection engine receives events from disparate servers and network devices, aggregates the information, and stores it into the event log. The enterprise event analyzer compares events from one enterprise to events from another enterprise (page 6, paragraph 0059);

an information processing/analyzing step performed by an information processing/analyzing section to collected security information and analyze the information using a predetermined analysis algorithm (page 6, paragraph 0059) as after the events have been consolidated and classified, they enter the correlation stage, which is performed by a hierarchy of event analyzers, which may include a plurality of network event analyzers, an enterprise event analyzer, preferably a part of the security subsystem, and a global event analyzer, preferably a part of the security master system. A network event analyzer analyzes data in various views, described above, looking for events exceeding predetermined thresholds. Event analyzers can also use the results of vulnerability scans to prioritize detected security events;

an information sharing/searching/announce step of managing processed and analyzed security information to be shared and searching for (0048) and providing the

information upon request (page 6, paragraph 0059) the enterprise event analyzer compares events from one enterprise to events from another enterprise; and an alerting step of sending predetermined early warning information to at least one of any inside and outside systems if an alert is required for any incident or vulnerability (page 6, paragraph 0060) as when an event is uploaded for review by the master system, a single ticket is generated for all security events determined to be related to the same attack and a security engineer begins researching the information in the ticket. Hrabik does not explicitly teaches analyzing the collected security information once its been put into a database. Hrabik appears to analyze the logs file and then place the processing results into a database. On the other hand, Gleichauf teaches the abovementioned limitation (column 2, lines 11-15) as the information from the collected banners is stored as entries in a first database. Analysis is performed on the entries in the first database by comparing the entries with a rule set to determine potential vulnerabilities. The results of the analysis are then stored in a second database.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Gleichauf into the system of Hrabik to provide better management options for the data collected from collection engine and analyzer engine.

As per claim 23, Hrabik teaches automatically protecting the integrated computer emergency response system's own information by using a predetermined information security section (0061; smart action).

With respect to claim 27, it is rejected in view of the same reasons as stated in the rejection of claim 16.

Claims 3, 5, and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hrabik et al. (US 2002/0178383 A1) in view of Gleichauf et al. (US 6,324,656 B1) as applied to claim 1 above, and further in view of Willebeek-LeMair et al. (US 7359962 B2).

With respect to claim 3, Hrabik teaches the limitation of "information collecting/managing section includes a vulnerability DB collecting unit for collecting, classifying and processing vulnerabilities" (page 6, paragraphs 0056 – 0057) as once the events have been received, the security system begins consolidating the events. To consolidate security events, each event is compared to a database of system and message "fingerprints" to properly identify the source of the event message. Once the log analyzer/event consolidator engine has uncovered the source of the event message, the system proceeds to classify the event by determining the overall meaning of the message and specific details necessary to make an evaluation of the significance of the event.

It is noted, however, that neither Hrabik nor Gleichauf explicitly teach the limitation of "vulnerabilities officially recognized and provided by various domestic or foreign company system hardware vendors and OS (operating system) vendors."

On the other hand, Willebeek-LeMair teaches the abovementioned limitation (Column 5, lines 20-36) as the system further includes a signature database that stores detection signatures (comprising, for example, security rules, policies and algorithms) that are designed to mitigate or avert network damage from detected vulnerabilities. These signatures may be obtained from any one of a number of well known sources, including, for example, machine (host) manufacturers, service suppliers, the Internet, and the like. Additionally, the signatures may be created by an administrator of the protected network. Still further, the signatures may be supplied by a entity in the business of signature creation, where that entity operates to collect threat information (for example, worm, virus, trojan, DoS, Access, Failure, Reconnaissance, other suspicious traffic, and the like) from around the world, analyze that information and design detection signatures that can be used by others to mitigate or avert network damage from the collected threats.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Willebeek-LeMair into the system of Hrabik and Gleichauf to improve the security of the system by providing wider range of device vulnerabilities that could be detected.

With respect to claim 5, it is noted that neither Hrabik nor Gleichauf explicitly teach the limitation of "information collecting/managing section includes an information security data collecting unit for collecting and storing information security data or references published by CERTs or ISACs, colleges, research centers and government

companies with respect to security incidents, including hackings, and countermeasure against the incidents, using an automated collecting tool, such as a web robot or a search engine."

On the other hand, Willebeek-LeMair teaches the abovementioned limitation (column 14, lines 34-42) as the vulnerability assessments generated by the network discovery functionality are presented to a network administrator, in detail or summary form, with enough information for the administrator to make a rapid, high level decision on responding to the vulnerability. The information provided to the administrator may include severity assessment and links to vendor patches and other pertinent data from the web that would assist in addressing the vulnerability.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Willebeek-LeMair into the system of Hrabik and Gleichauf to provide for administrator additional tools to resolve the system vulnerabilities.

With respect to claim 6, it is noted that neither Hrabik nor Gleichauf explicitly teach the limitation of "information collecting/managing section includes a virus/worm information collecting unit for collecting and storing information about computer viruses or worms using an automated collecting tool, such as a virus alert system, an agent or a search engine."

On the other hand, Willebeek-LeMair teaches the abovementioned limitation (column 10, lines 36-41) as a threat aggregation functionality stores threat information

(for example, worm, virus, trojan, DoS, Access, Failure, Reconnaissance, other suspicious traffic, and the like) collected from around the world.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Willebeek-LeMair into the system of Hrabik and Gleichauf to provide for administrator additional tools to resolve the system vulnerabilities.

Claims 12, 18, 19, and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hrabik et al. (US 2002/0178383 A1) in view of Gleichauf et al. (US 6,324,656 B1) as applied to claims 1, 2, and 22 above, and further in view of Hutchinson et al. (US 2003/0233438 A1).

With respect to claim 12, it is noted that neither Hrabik nor Gleichauf explicitly teach the limitation of "information sharing/searching/announce section has a profile management function of classifying information to be shared according to types or classes and users/companies who will share information according to classes and a information providing function for receiving a user's request for information search and providing the requested information to the user's system."

On the other hand, Hutchinson teaches the abovementioned limitation as (page 4, paragraph 0041) as based on a verification and/or authentication of a user, and further based on the user's account (e.g., user profile, privileges, etc.), a Framework Server can provide one or more interfaces through which the user can, for example,

create, search, view, and edit policies, configuration standards, asset profiles, vulnerability profiles, and risk assessment questionnaires for an associated Enterprise.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Hutchinson into the system of Hrabik and Gleichauf to provide a convenient way for a user to access and manage enterprise assets.

With respect to claim 18, Hrabik teaches (page 3, paragraph 0025) a configuration ensuring that the integrity of the master system can not be undermined.

In addition, Hrabik teaches the limitation of "a network/system/document security unit including at least one of a PKI certification system, an intrusion detection system, an anti-virus system, a retracing system and a watermarking system" (FIG. 2; page 3, paragraph 0039) as at least one of the security subsystems, each of the security subsystems connected to IDS servers, workstations, firewall, and routers for detecting if security is compromised.

It is noted, however, that neither Hrabik nor Gleichauf explicitly teach the limitation of "a physical information security unit including at least one of a card certification unit, a password certification unit, a biometrics unit and a CCTV."

On the other hand, Hutchinson teaches the abovementioned limitation (page 4, paragraph 0038) as a Framework Server can include instructions for providing interfaces to provide access to the stored information, where (page 4, paragraph 0041) the interface can be encoded in a wide variety of instruction sets/data user can enter or

otherwise provide a user identifier (e.g., Login Name and Password) and (page 3, paragraph 0035) a user identifier is defined as a login name and password, a fingerprint, a voice sample etc.

It would have been obvious to incorporate teachings of Hutchinson into the system of Hrabik and Gleichauf to allow user to access, examine, and edit the asset and vulnerability information stored in the system in a secure manner.

With respect to claim 19 in view of claim 2, Hrabik teaches (page, paragraph 0059) the enterprise event analyzer compares events from one enterprise to events from another enterprise, allowing their true nature and significance to be understood.

It is noted, however, that neither Hrabik nor Gleichauf teach the limitations of "an information management unit for processing, analyzing and taking statistics on information to be exchanged with external systems in an encrypted standard format and classifying companies according to user classes" and "an interface for performing an access control (providing data according to user classes) and a protocol conversion for data exchange with external systems."

On the other hand, Hutchinson teaches the abovementioned limitation of "an information management unit for processing, analyzing and taking statistics on information to be exchanged with external systems in an encrypted standard format" (page 6, paragraph 0049) as a Framework Server can track or otherwise monitor vulnerabilities from a variety of sources, such as mailing lists, internet web sites, and information disseminated by others (e.g., hackers). When a Framework Server detects

a vulnerability (e.g., update of an existing vulnerability, new vulnerability), the vulnerability module can identify the vulnerability, provide a numerical vulnerability risk rating ranging from, for example, one to ten based upon impact (i.e., the results of a vulnerability being exploited), popularity (i.e., how well-known a vulnerability is in the community), and simplicity (i.e., the level of technical expertise required to exploit a vulnerability), classify the vulnerability type (e.g., exploitable remotely and/or locally), archive the vulnerability source code, identify one or more assets and/or asset components that can be affected by the vulnerability, and/or provide a link (e.g., a uniform resource locator) to a patch. Furthermore, (page 8, paragraph 0062) copies of Framework Server data, may be transmitted by a secure channel using a secure communications technique, to an Account Server that may store a backup of a Framework Server.

In addition, Hutchinson teaches the limitation of "classifying companies according to user classes" (Fig. 8; page 8, paragraph 0064) as an Account Server may determine associated privileges for a Framework Server incorporated into the intranet or other network within which the Enterprise exists, where such privileges can be based on an Enterprise Account. Hutchinson further teaches an Enterprise Account (page 8, paragraph 0062) as data associated with an Enterprise such as assets, asset components, asset profiles, functional units, user accounts, configuration standards, and other components.

Finally, Hutchinson teaches the limitation of "an interface for performing an access control (providing data according to user classes) and a protocol conversion for

data exchange with external systems" (page 8, paragraph 0064) as the Account Server may optionally provide an interface to an Enterprise/Framework Server via the internet such that the Framework Server can communicate to the Account Server to obtain updates on configuration standards, vulnerabilities, and other data. A Framework Server may establish a secure channel (e.g., anonymous SSL) with an Account Server where a Framework Server can "log-in" or otherwise establish communications with the Account Server such that the Account Server can verify an Enterprise with which a Framework Server can be associated. Based on such association of Enterprise and Framework Server, an Account Server may determine associated privileges for a Framework Server, where such privileges can be based on an Enterprise Account. Furthermore, (page 9, paragraph 0066) upon a valid and/or authenticated request from a Framework Server, an Account Server may query vulnerability data (e.g., profiles) to which the Account Server has access, to determine which vulnerability data may be applicable to the requesting Framework Server.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Hutchinson into the system of Hrabik and Gleichauf to provide an easy way to access the data specific to Enterprise Vulnerabilities Data based on Enterprise specific parameters.

With respect to claim 24, it is rejected in view of the same reasons as stated in the rejection of claim 19.

Claims 13-15, 25, and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hrabik et al. (US 2002/0178383 A1) in view of Gleichauf et al. (US 6,324,656 B1) as applied to claims 2 and 22 above, and further in view of Hill et al. (US ,088,804).

With respect to claim 13, it is noted that neither Hrabik nor Gleichauf explicitly teach the limitation of "an attack assessment section for performing attack assessments for security incidents, such as hackings or cyber terror, classifying the incidents based on past attack methods and frequencies, supplying possible attack scenarios and automatically implementing attack assessment functions, including databasing of vulnerability analysis results, real-time analysis of critical attacks, collection and analysis of important packets and issuance and spread of a forecast/warning, in a pre-defined manner."

On the other hand, Hill teaches the abovementioned limitation (column 9, lines 35-45) as a task 116 predicts a pattern for subsequent attacks and adapts security system to respond to subsequent attacks. Security system is adapted by introducing first attack signature into security system as a new training signature and repeating training process. The result of introducing first attack signature as a new training signature, and mapping a vector representative of the new training signature into display map, is an improved response to subsequent attacks that have subsequent training signatures that most closely resemble first attack signature.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Hill into the system of Hrabik and Gleichauf to provide a way for the security system to evolve with evolving threats.

With respect to claim 14, it is noted that neither Hrabik nor Gleichauf teach the limitation of "a test-bed for supplying a possible scenario when a new security incident or vulnerability is detected and performing a simulation under the same condition of a system to be protected so that an attack level and any damage and effective response can be expected."

On the other hand, Hill teaches the abovementioned limitation (column 2, line 66 – column 3, line 2) as training the security system to respond to a plurality of training signatures, each of the training signatures representing one of a plurality of simulated attacks, where (column 5, lines 39-40) each of simulated attacks is a prediction of an attack type that may occur on the network, and (column5, lines 31-38) an attack is defined as a plurality of security events occurring substantially concurrently in a given sampling period at a plurality of nodes. The sampling period is an arbitrary amount of time that is of a sufficient length to receive enough security events to form an attack signature for an attack.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Hill into the system of Hrabik and Gleichauf to provide a way for the security system to evolve with evolving threats.

With respect to claim 15, it is noted that neither Hrabik nor Gleichauf teach the limitation of "an early forecast/warning section for generating an alert signal to the results issued by the test-bed or attack assessment section and sending the alert signal to a system to be protected or an external system to inform of any security incident or vulnerability."

On the other hand, Hill teaches the abovementioned limitation (column 8, line 55-58) as the mitigation list may be generated during training process or at any other time by a network administrator after evaluating various training attack scenarios.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Hill into the system of Hrabik and Gleichauf to provide a comprehensive guide to resole various security issues.

With respect to claim 25 in view of claim 22, it is rejected in view of the same reasons as stated in the rejection of claim 13.

With respect to claim 26 in view of claim 22, it is rejected in view of the same reasons as stated in the rejection of claim 14.

Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hrabik et al. (US 2002/0178383 A1) in view of Gleichauf et al. (US 6,324,656 B1) and Hill et al. (US 6,088,804) as applied to claim 14 above, and further in view of Hutchinson et al. (US 2003/0233438 A1).

With respect to claim 17, it is noted that neither of Hrabik, Gleichauf, and Hill explicitly teach the limitation of "an automatic education/training section for generating educational information from the results of a simulation performed at the test-bed, storing and managing the educational information and sending the educational information to an external terminal that requires education."

On the other hand, Hutchinson discloses the abovementioned limitation (page 1, paragraph 0008) as generating at least one vulnerability profile that can be associated with at least one detected vulnerability of an asset(s), where the vulnerability profile(s) can include at least one link to one or more software patches and/or other information associated with the vulnerability. A user(s) can be notified of the generated vulnerability profile.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Hutchinson into the system of Hrabik, Gleichauf, and Hill to provide additional tools for a user to address the system vulnerabilities.

Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hrabik et al. (US 2002/0178383 A1) in view of Gleichauf et al. (US 6,324,656 B1) and Willebeek-LeMair et al. (US 7359962 B2) as applied to claim 3 above, and further in view of Schneier et al. (US 2002/0087882 A1).

With respect to claim 20, Hrabik teaches the limitation of "a vulnerability DB for storing a list of various vulnerabilities of relevant systems and a vulnerability checking

list" (Fig. 4; page 6, paragraph 0056) as a database of system and message "fingerprints."

Further, Hrabik teaches the limitation of "a blacklist DB for selecting habitually occurring incidents from the list of vulnerabilities and security incidents and storing the habitual incidents" (page 6, paragraph 0057) as the database of event-message types that holds trending information regarding the types of events occurring most often.

It is noted, that Hrabik does not explicitly teach the limitations of "a source/processed DB for storing source data and processed data of collected security information", "a reported incident DB for storing incident information inputted through the incident report collecting section", "an alert DB for selecting incidents about which an early forecast or alert is required from the list of vulnerabilities and security incidents and storing the selected incidents", "a profile DB for storing information about relevant systems and users", and "an incident history DB for storing previous incidents and vulnerabilities, together with countermeasure against such incidents and vulnerabilities and various log files."

On the other hand, Gleichauf teaches the limitation of "a source/processed DB for storing source data and processed data of collected security information" (Fig. 1; Abstract) as a Port database holding information resulting from the port scans and Datamine database holding the results of analysis of the Port database.

Furthermore, Willebeek-LeMair teaches the limitation of "a profile DB for storing information about relevant systems and users" (column 5, lines 9-15) as the system includes an enterprise resource database containing enterprise specific data identifying

machines in the network, services provided by the host, and potential computer system and network device vulnerabilities associated with those machines and services in the context of the network configuration.

It is further noted that neither of Hrabik, Gleichauf, and Willebeek-LeMair teach the limitations of "a reported incident DB for storing incident information inputted through the incident report collecting section", "an alert DB for selecting incidents about which an early forecast or alert is required from the list of vulnerabilities and security incidents and storing the selected incidents", and "an incident history DB for storing previous incidents and vulnerabilities, together with countermeasure against such incidents and vulnerabilities and various log files."

However, Schneier teaches the abovementioned limitations of "a reported incident DB for storing incident information inputted through the incident report collecting section" and "an alert DB for selecting incidents about which an early forecast or alert is required from the list of vulnerabilities and security incidents and storing the selected incidents" (Fig. 4; page 6, paragraph 0085) as Problem/Event database that stores the event records created from the gateway messages where (page 8, paragraph 0116) the severity of the gateway message/event can be evaluated based on some threshold.

Finally, Schneier teaches the limitation of "an incident history DB for storing previous incidents and vulnerabilities, together with countermeasure against such incidents and vulnerabilities and various log files" (Fig 4;page 6, paragraph 0086) as

Problem/event resolution database that can include, among other things, a database of vulnerabilities.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Schneier into the system of Hrabik, Gleichauf, and Willebeek-LeMair to provide an efficient way to track the network problems and events.

Claim 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hrabik et al. (US 2002/0178383 A1) in view of Gleichauf et al. (US 6,324,656 B1) and Willebeek-LeMair et al. (US 7359962 B2) as applied to claim 3 above, and further in view of Aaron et al. (US 2003/0188191 A1).

It is noted that neither of Hrabik, Gleichauf, and Willebeek-LeMair explicitly teach the limitation of "a computer forensic DB for extracting information about events recognized as computer crimes from records of attacker IP addresses which were or can be origins of critical attacks and storing the extracted information for use as evidence later when a victim of a security attack files a criminal complaint or a civil action, seeking compensation for any financial damages or losses."

On the other hand, Aaron teaches the abovementioned limitation (page 5, paragraph 0052) as a central database where data records comprise a time-stamp, a description of the activity, and the source of the probe.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Aaron into the system of Hrabik, Gleichauf, and Willebeek-LeMair to collect the information relevant to the source of the intrusion.

Claim 21 is also rejected under 35 U.S.C. 103(a) as being unpatentable over Hrabik et al. (US 2002/0178383 A1) in view of Gleichauf et al. (US 6,324,656 B1) and Willebeek-LeMair et al. (US 7359962 B2) and Schneier et al. (US 2002/0087882 A1) as applied to claim 20 above, and further in view of Aaron et al. (US 2003/0188191 A1).

It is noted that neither of Hrabik, Gleichauf, Willebeek-LeMair, and Schneier explicitly teach the limitation of "a computer forensic DB for extracting information about events recognized as computer crimes from records of attacker IP addresses which were or can be origins of critical attacks and storing the extracted information for use as evidence later when a victim of a security attack files a criminal complaint or a civil action, seeking compensation for any financial damages or losses."

On the other hand, Aaron teaches the abovementioned limitation (page 5, paragraph 0052) as a central database where data records comprise a time-stamp, a description of the activity, and the source of the probe.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Aaron into the system of Hrabik, Gleichauf, Willebeek-LeMair, and Schneier to collect the information relevant to the source of the intrusion.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is (571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am - 5:00pm, EST. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R. V./

Examiner, Art Unit 2431

/Ayaz R. Sheikh/
Supervisory Patent Examiner, Art Unit 2431